REMARKS

Applicants have carefully reviewed and considered the Examiner's Action mailed June 26, 2007, in which the subject matter of claims 20-28 were indicated as being allowable over the prior art of record, if rewritten in independent form. Reconsideration is respectfully requested in view of the foregoing amendments and the comments set forth below.

By this Amendment, claims 1-3, 9-11, 13, 16, 18, 24 and 26-27 have been amended. No claims have been added or canceled. Consequently, claims 1-35 remain pending in the present application, with claims 20-28 being indicated as containing allowable subject matter.

In particular, independent claims 1, 10, and 11 are amended in order to clarify that the claimed invention includes a first feature: "used for a case where n first shares are generated from original secret information, n being an integer equal to or greater than two, by using a first threshold secret sharing scheme, in which the original secret information can be reconstructed by a collection of at least any k members from a group having n members ($2 \leqq k \leqq n$), and the n shares are distributed to the n members," and a second feature: "each member among the collected t members uses a second secret sharing scheme, in which original secret information can be reconstructed by a collection of t members from the collected t members, to generate t second shares from its first share, and distributes one second share to each member among the t members including itself."

The first feature is supported, for example, as a (k, n) threshold secret sharing scheme by page 21, lines 23-27 in the present specification (i.e., paragraph 0092 in the

publication US 2004/0179686 A1). The second feature is supported, for example, as a (k', t) threshold secret sharing scheme by page 26, lines 11-14 in the present specification (i.e., paragraph 0105 in the publication US 2004/0179686 A1) and page 52, lines 1-2 in the specification (i.e., paragraph 0169 in the publication US 2004/0179686 A1). The attached exemplary Figure A illustrates the claimed invention.

Claims 1-8, 10-17 and 29-34 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,810,122 to Miyazaki et al. (hereinafter referred to as "Miyazaki"). Claims 9, 18 and 19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Miyazaki in view U.S. Patent Application Publication No. 2003/0046202. These rejections are respectfully traversed.

In contrast to the claimed invention set forth in independent claims 1, 10 and 11, Miyazaki discloses a secret sharing system and storage medium where, when each shareholder Pi holds (n,n) share di about a secret key d, all the shareholders P1 to Pn shares di in the form of (t,n) partial random-number information and each of the shareholders P1 to Pn puts together pieces of the partial random-number information for each digit to create partial information $d_{j,k}$. See column 8, lines 3-9 of Miyazaki. At most, Miyazaki relates to a case where n first shares are generated from original secret information by using a (n, n) threshold secret sharing scheme as a first secret sharing scheme and the n first shares are distributed to the n members, and which includes a step of generating a (t, n) partial-number information in a second secret sharing scheme. The attached exemplary Figure B schematically illustrates the secret sharing scheme of Miyazaki.

As can be understood by comparing exemplary Figure A with exemplary Figure B and as described above, Miyazaki discloses a method, the first secret sharing scheme of which is always a (n, n) threshold secret sharing scheme, and does not disclose the above-mentioned first feature of independent Claims 1, 10, and 11 of the present application, i.e., a (t, n) threshold secret sharing scheme.

In addition, as can be understood by comparing exemplary Figure A with exemplary Figure B and as described above, Miyazaki discloses a method, the second secret sharing scheme of which is always a (t, n) threshold secret sharing scheme, and does not disclose the above-mentioned second feature of independent Claims 1, 10, and 11 of the present application, i.e., a (t, t) threshold secret sharing scheme.

Accordingly, the above-identified first and second features of independent Claims 1, 10, and 11 of the present application are not disclosed in Miyazaki. Consequently, Miyazaki cannot anticipate the claimed invention because it fails to disclose each and every recited feature in the claims. Withdrawal of the rejection under 35 U.S.C. §102(e) is respectfully requested.

Knapp is directed to an anonymous transactions between an entity and a provider and is applied for its disclosure of "generating third shares from the member IDs of the t members by using a secret sharing scheme (Fig. 3,[0019] lines 14-34) and distributing them to the t members (Fig. 3 [0019] lines 14-34, [0022] lines 28-36)." Nowhere does Knapp provide a disclosure or teaching of the first and second features that are missing from Miyazaki. Accordingly, even if combined, the claimed invention would not result. Withdrawal of the rejection of claims 9 and 18-19 under 35 U.S.C. §103(a) is respectfully requested.

In view of the foregoing amendments and remarks, it is respectfully requested that the rejections of record be withdrawn and that a Notice of Allowance be issued indicating that claims 1-35 are allowed over the prior art of record.

Should the Examiner believe that a conference would advance the prosecution of this application, the Examiner is encouraged to telephone the undersigned counsel to arrange such a conference.

Respectfully submitted,

Date: November 20, 2007

Catherine M. Voorhees
Registration No. 33,074
VENABLE LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300

CMV/elw
::ODMA\PCDOCS\DC2DOCS1\909782\1